AFRL-AFOSR-UK-TR-2014-0049

Random Matrix Theory and Elliptic Curves

Jonathan P. Keating

THE UNIVERSITY OF BRISTOL
SENATE HOUSE, TYNDALL AVENUE
BRISTOL, BS8 1TH, UNITED KINGDOM

EOARD Grant 10-3088

Report Date: November 2014

Final Report from 1 October 2010 to 30 September 2014

Air Force Research Laboratory
Air Force Office of Scientific Research
European Office of Aerospace Research and Development
Unit 4515, APO AE 09421-4515

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11/24/2014	Final	1 October 2010-30 September 2014

4. TITLE AND SUBTITLE
Random Matrix Theory and Elliptic Curves

5a. CONTRACT NUMBER
FA8655-10-1-3088

5b. GRANT NUMBER
Grant 10-3088

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Keating, Jonathan P.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
THE UNIVERSITY OF BRISTOL
SENATE HOUSE, TYNDALL AVENUE
BRISTOL, BS8 1TH, UNITED KINGDOM

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
EOARD
Unit 4515
APO AE 09421-4515

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR/IOE (EOARD)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-UK-TR-2014-0049

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This grant focused on the use of random matrix theory (RMT) to understand the zeros of L-functions, in the context of the statistical properties of elliptic curves and arithmetic statistics. The rank of a curve (an integer describing the number of rational points on the curve) is relevant to cryptography; this work showed relations between RMT and classification of elliptic families based on L-functions. The second function of the grant is the application of RMT to determine statistical properties of the prime numbers, of great relevance to cryptography. The team was able to prove two long-standing conjectures (Hooley 1974, Goldston/Montgomery 1984) and computed formulae related to the intervals of prime numbers.

15. SUBJECT TERMS
EOARD, Random Matrix theory, Riemann Hypothesis, Elliptic Curves

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			PUTZ, VICTOR
UNCLAS	UNCLAS	UNCLAS	SAR	12	19b. TELEPHONE NUMBER *(Include area code)* 2356013

Final Report on EOARD Grant 103088 (Random Matrix Theory and Elliptic Curves)

J.P. Keating and N.C. Snaith

November 24, 2014

L-functions encode information about a range of quantities of fundamental importance in number theory. In the cases of the Riemann zeta function and Dirichlet L-functions, this information relates to the prime numbers, but there are also L-functions associated to elliptic curves, modular forms and a range of other objects, allowing investigation using analytic techniques. As an indication of their significance, two of the Clay Millennium Prize Problems, the Riemann Hypothesis and the Birch–Swinnerton-Dyer Conjecture, are related to L-functions. Moreover, the objects they describe – the primes and elliptic curves – play a central role in cryptography.

Many recent advances in the study of L-functions have been prompted by insight from random matrix theory (RMT). The key to this connection is the distribution of the complex zeros of the Riemann zeta function $\zeta(\frac{1}{2}+it)$, and other L-functions, that the Riemann Hypothesis places on the critical line (where t is real). Evidence has mounted since the 1970s that in a suitable asymptotic regime these zeros show the same statistical behaviour as the eigenvalues of random unitary matrices. For example, the characteristic polynomial of a random matrix, which has zeros at the eigenvalues of that matrix, has been found to be a good model for predicting value distributions of L-functions (see work of Keating and Snaith [24, 23]). Through this analogy, RMT has proved to be of central importance in predicting values of individual L-functions averaged up the critical line, for example,

$$\frac{1}{T}\int_0^T \left|\zeta\left(\frac{1}{2}+it\right)\right|^{2k} \mathrm{d}t, \tag{1}$$

and also values averaged over families of naturally related L-functions at a fixed height on the critical line [23], since zero statistics averaged over families are also believed to be described by RMT as in the work of Katz and Sarnak [19]. The link with random matrices is, however, still a conjecture (albeit one supported by considerable experimental evidence). Understanding this link is one of the great challenges of the subject.

In the reverse direction, knowing that the zeros of an L-function are random-matrix distributed should tell us about correlations between the objects the L-function counts. For example, knowing that the zeros of the Riemann-zeta-function are random matrix distributed should tell us something about the statistical distribution of the primes, and knowing this for the L-functions associated with elliptic curves should tell us about the fluctuations in the number of rational solutions. In general, fluctuations in number-theoretic quantities such as those just described are known as *arithmetic statistics*.

In the case of function fields, where the role of the primes is played by irreducible polynomials defined over finite fields, the analogue of the Riemann Hypothesis is known to be true (by work of Weil). It has also been proved, by Katz and Sarnak [19], that the zeros of the corresponding L-functions are distributed like the eigenvalues of random matrices in the limit of large finite field.

The key aims of the grant were to use random matrix theory to understand better

- the statistical properties of elliptic curves
- arithmetic statistics

1 Elliptic Curves and their L-functions

This grant funded what we consider to be a particularly interesting application of RMT to families of L-functions associated to elliptic curves. The rank of a curve is an integer that describes the number of rational

points on that curve. Counting rational points on curves is a field with a rich history and significant potential impact in applications to the internet and security. Much is still unknown about the relative frequency of ranks in families of elliptic curves. When elliptic curves are gathered into natural families it is not known what proportion of the family has a given rank, or even if there is a maximum rank associated to the family. These questions have have engaged the minds of the leading mathematicians of the past 100 years, including in the current generation: a case in point being the recent work on the average rank of elliptic curves by Bhargava and Shankar. Bhargava won one of the 2014 Fields Medals.

These are questions naturally suited to random matrix techniques, which provide conjectures for averages over such families of elliptic curves via their associated L-functions. This investigation was started in 2002 by Conrey, Keating and Rubinstein and Snaith [11]. We used random matrix theory to predict the number of L-functions, in a family associated to elliptic curves, that have a zero in the complex plane at the point 1/2. While the total number of L-functions in the family is proportional to a parameter T, the number of L-functions that take the value zero at 1/2 is conjectured, asymptotically for large T, to be proportional to $T^{3/4}(\log T)^{3/8}$. This family contains only L-functions associated to elliptic curves with even rank (0,2,4,6, etc) and this result is important because, by the Birch–Swinnerton-Dyer conjecture, counting L-functions that are zero at the central point $s = \frac{1}{2}$ is the same as counting elliptic curves with even rank greater than or equal to two. There is recent and convincing numerical evidence [12] for the powers of T and $\log T$. It is particularly noteworthy that before we introduced RMT as a method to predict the rank distribution there was no method to determine the correct power of $\log T$.

The need for a further refinement of the RMT model for elliptic curve L-functions became clear when a rather striking mystery arose with the publication by S.J. Miller [27] of some numerical results for statistics of zeros of elliptic curve L-functions with a relatively small parameter T. Although it is known that convergence to a limit as T increases is infamously slow in these families, the statistics observed by S.J. Miller were completely unexpected in that they are qualitatively different from the RMT $SO(2N)$ limit expected for large conductor: they show significant "repulsion" of zeros from the central point. Figure 1 shows this repulsion (in the drop to zero near the origin) for a family of elliptic curve L-functions. The repulsion is not predicted by even the "ratios conjectures", which are the best means yet of predicting the statistics away from the origin. In Figure 1 we see the repulsion at the origin and also observe that the amount of repulsion decreases as the parameter T increases. This suggests that, as expected, in the $T \to \infty$ limit the data will tend to $SO(2N)$ statistics as predicted by Katz and Sarnak.

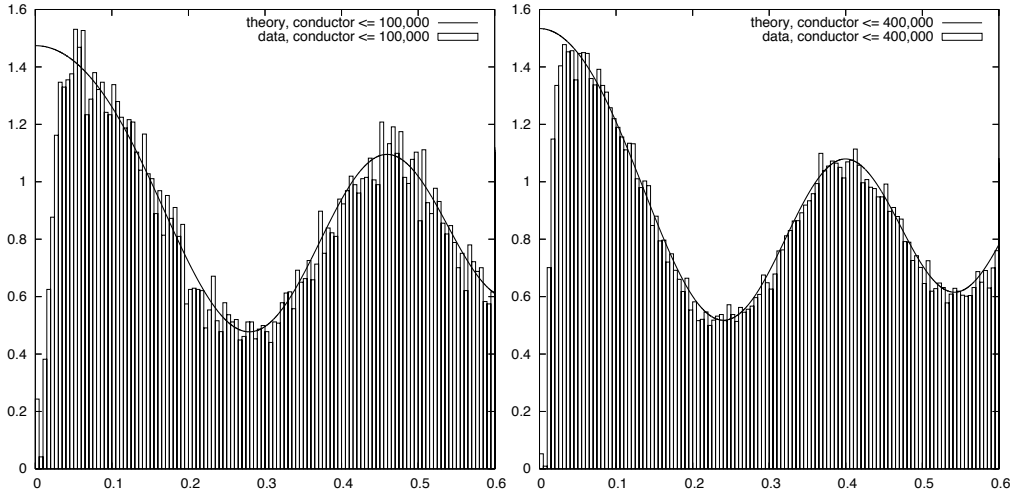

Figure 1: 1-level density of unscaled zeros (that is, a histogram of the distances from the central point of the zeros on the critical line) from 0 up to height 0.6 for a family with $T = 100,000$ *left* and $T = 400,000$ on the *right* hand side, prediction (solid line), from the ratios conjecture, versus numerical data (bar chart).

However, it became clear with the publication of S.J. Miller's numerics that a significantly more refined model than just $SO(2N)$ was needed to predict the statistics of zeros of elliptic curve L-functions near the central point $\frac{1}{2}$ for relatively small parameter T. Investigation of this problem by Dueñez, Huynh, Keating, S.J. Miller and Snaith was funded by this grant and culminated in the publication of [15]. The research suggests that it is the discretization of the values of the L-functions at the point $\frac{1}{2}$ which is responsible for the repulsion S.J. Miller observed. Work of Waldspurger [32], Shirmura [31] and Kohnen–Zagier

[25] implies that a non-zero value below a cut-off $C(T)$ is never observed for the value of the L-functions at the central point. Values of zero at the central point are expected to correspond to curves of rank higher than zero. Thus the value of the L-function of a rank 0 curve is discretized and cannot take on arbitrarily small positive values. This in turn appears to imply that zeros of the L-function close to the point $\frac{1}{2}$ are less likely than would be expected otherwise, which explains the "repulsion" discovered by Miller. While as T becomes large this discretization becomes smaller and has less and less effect on the zero statistics (which in the limit are believed to show $SO(2N)$ statistics), for the relatively small values of T at which we do numerical computation this discretization is important. We model this using an "excised" random matrix model. Let A be a matrix from $A \in SO(2N)$ with eigenvalues $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_N}$ and characteristic polynomial, $\Lambda_A(s) = \prod_{j=1}^{N}(1 - se^{i\theta_j})(1 - se^{-i\theta_j})$. In the excised model for rank 0 curves, we average only over those matrices for which $\Lambda_A(s)$ at $s = 1$ (modelling the values of the L-functions at the point $\frac{1}{2}$) takes values greater than some cut-off value X. Comparing with the dependence of $C(T)$ on T in the number theory case we can predict, for the family of L-functions in Figure 1, that $X = 2.188 \exp(-\frac{N}{2})$. Generating matrices from $SO(2N)$ numerically, we have the picture in Figure 2 for the cumulative distribution of the positions of the first zero above $\frac{1}{2}$ the L-functions in a family with $T = 400000$ and see that the red excised model curve captures the novel repulsion from the point $\frac{1}{2}$ that we seek to understand.

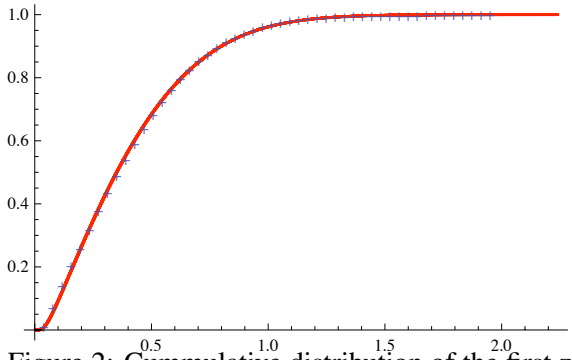

Figure 2: Cummulative distribution of the first zero of the family of even quadratic twists of E_{11} for prime discriminant up to 400 000 (blue crosses) and numerically generated eigenvalues from the excised model (red line)

The grant also funded the work of summer undergraduate students and a PhD student who investigated the L-functions associated to higher rank elliptic curves. The zero statistics in the previous paragraphs are for elliptic curves of rank zero, but we have also been working on understanding the zero statistics of curves of ranks 1 and 2. The ultimate goal of this would be to predict the number of elliptic curves in a family with rank higher than 1 or 2, an extension of the Conrey, Keating, Rubinstein, Snaith work predicting the number of curves with rank higher than 0. We have made good progress towards this by understanding the zero statistics of L-functions associated to elliptic curves of rank 2 or higher, and in investigating the equivalent discretisation of values phenomenon for rank 1 curves. This work is in progress and being prepared for publication.

A related strand of work aims to write down precise expressions describing the statistics of the zeros of either a single L-function, or a natural family of L-functions. Long-standing results in random matrix theory show that the n-point correlation functions (in some situations these are also called n-level densities) of eigenvalues from ensembles of random matrices such as $U(N)$, $SO(N)$ and $USp(2N)$ can be written concisely as n-dimensional determinants of matrices whose elements are the kernel belonging to the particular ensemble (see, for example, [9] where the kernels and correlation functions are written down for these groups). These results are elegant and exact, and their determinantal form is very useful for calculations within random matrix theory (RMT). However, the corresponding quantity in number theory, the n-point correlation function (or level density) of the complex zeros of an L-function, or of families of L-functions, does not seem to take this concise determinantal form, except in a suitable asymptotic limit where the statistics are expected to agree with RMT. This leads us to a question: is there a different, albeit less elegant, way to write the random matrix eigenvalue correlation functions that might help to make precise conjectures about the form of the correlations of zeros? Furthermore, given that the determinantal form is not available in the number theory case, is there a natural form in which to write the n-correlations of the zeros that is useful for further applications? These questions have been answered by Conrey and Snaith [14] in the case of

the Riemann zeta function, which has zeros displaying the statistics of eigenvalues of matrices from $U(N)$, with Haar measure, in the appropriate limit. They show that the form of the n-point correlation function resulting from the method using the average of ratios of characteristic polynomials allows for immediate simplification when the support of the test function is restricted - something that is critical for comparison with rigourous results in number theory and something that is certainly not true of the determinantal form. This allows them to apply to the n-point correlation function for eigenvalues from $U(N)$ the same restriction to the support of the test function that was used by Rudnick and Sarnak in [30] when looking at the n-point correlation function for zeros of a general L-function. Then the identical structure of the two expressions reveals that they coincide in their respective asymptotic limits.

The above work was funded by the current grant, and it lead to a further project, aimed at answering the same two questions above in the case of families of L-functions. In recently submitted work by A.M. Mason and Snaith [26], the n-level density functions of eigenvalues from matrices in $SO(2N)$ were calculated using averages of ratios of characteristic polynomials. The steps were then repeated using the ratio conjecture for a family of L-functions associated with elliptic curves. The zeros of this family are expected to behave statistically like the eigenvalues of $SO(2N)$. The ratio conjecture was used to derive the n-level densities of zeros of the L-functions in this family, complete with lower order terms. Similarly, eigenvalues of matrices from $USp(2N)$ are considered in the same way, and Mason and Snaith demonstrate the method with a family of L-functions showing symplectic symmetry. It was found that, as in the case of the Riemann zeta function, the resulting expressions are in the perfect form for comparison with rigourous results in number theory where there is a restriction on the support of the test function that selects which zeros contribute to the statistics.

There are some well-studied families of L-functions that have been thoroughly investigated with regards to their connection with random matrix theory. In [13], Conrey and Snaith investigate a more unusual family to see if random matrix statistics are seen here also. L-functions are fundamental objects in number theory that carry a lot of arithmetic information. Probably the most famous example is the Birch and Swinnerton-Dyer conjecture that equates the rank of an elliptic curve with the order of vanishing of its L-function at the central point. It is generally believed that the vanishing of an L-function at its central point indicates some arithmetic-geometric structure. There are many theorems concerning the first-order vanishing of elliptic curve L-functions and random matrix theory has been used to model the frequency of second-order vanishing [11], as described above. In addition, the Langlands philosophy predicts that for any L-function arising from an automorphic representation there is a new L-function associated with the rth symmetric power representation. Combining these ideas, Barry Mazur asked the following question: Given the L-function of an elliptic curve $E/\mathbb{Q}$, is it true that the central value of the L-function of its nth symmetric power vanishes, if ever, for at most finitely many values of n? He admitted that it would likely be too difficult to answer this question, but further asked if random matrix theory could provide a model for this question.

Conrey and Snaith investigated this interesting question in a related family of L-functions. It seems that these L-functions do form an orthogonal family, and we can model this family using random matrix theory. They take some theoretical steps and in particular can prove an asymptotic formula, with power savings, for the first moment of the L-functions in this family. This improves an asymptotic formula with no error term proven by Greenberg [18] and Villegas–Zagier [28]. They can also give an upper bound that is probably too large by only one logarithm for the second moment of the L-functions in this family. They conclude, by Cauchy's inequality, that at least $N/(\log^2 N)$ of the first N L-functions in this family do not vanish at their central point. Moreover, assuming that the Riemann Hypothesis holds for this family, then they can compute the one-level density for this family, from which it follows that at least $1/4$ of the L-functions in this family do not vanish at their central point.

2 Arithmetic Statistics

The second goal set out in our proposal was to apply ideas from Random Matrix Theory to determine statistical properties of the primes. This is a novel idea in that it reverses the usual direction of travel. In [21] we achieved this in a key example: we were able to prove two long-standing conjectures, one due to Hooley in 1974 and the other due to Goldston and Montgomery in 1984, concerning the distribution of the primes in the context of irreducible polynomials in function fields defined over finite fields. Specifically, we

were able to compute formulae for the variances of the irreducible polynomials falling in short intervals in terms of the interval size, and in arithmetic progressions in terms of the modulus. We see this as a major step forwards. Our approach relies on relating the variances to sums over characters, and then using the Deligne equidistribution theorems to relate these sums to matrix integrals, which could then be evaluated.

We have subsequently extended this research programme to the variances of other important arithmetic functions, including the (generalised) divisor function (which counts the number of divisors), the Möbius function (which counts the number of prime factors), and the square of the Möbius function (which counts square-free numbers). This required a number of interesting new matrix integrals to be evaluated. We were able to prove in the function-field setting the analogues of several well-known conjectures, including the Good-Churchhouse conjecture (1968). A paper on the Möbius function and squarefrees with Zeev Rudnick has been completed [22]; a second paper on divisor functions with Edva Roditty-Gershon, Brad Rodgers and Zeev Rudnick is close to completion.

As a corollary of our results, we have also made interesting progress in proving the analogue of the Hardy-Littlewood conjecture in the function-field setting for large finite fields. Put forward by Hardy and Littlewood in 1923, this is one of the central conjectures in number theory. For example, it quantifies the twin-prime conjecture, that there are infinitely many pairs of primes separated by 2 (e.g. 17 and 19, 29 and 31, etc.) by giving a formula for the expected density of twin-primes. Furthermore it extends this to all separations, not just 2. Recently Lior Bary-Soroker proved the analogue of the Hardy-Littewood conjecture for function fields to leading order in the size of the finite field over which the polynomials are defined, in the limit as this size tends to infinity. However, at the leading order he calculates one loses all dependence on the separation – the irreducible polynomials are uncorrelated in this limit. The key challenge has been to understand the correlations which are contained in the lower-order terms. At a meeting at the CRM in Montreal earlier this year, this was identified as a major problem, but the general consensus was that current techniques were insufficient to say anything about it. Recently, Edva Roditty-Gershon and JPK have shown that this is not the case: we have proved formulae for the average of the lower-order terms that captures significant information about the correlations. Our approach uses the method developed in [21]. A paper is currently in preparation. Probing the Hardy-Littlewood conjecture was one of our most ambitious objectives and we are very pleased to have been able to make this progress.

Related to this we also established the corresponding formula we need to carry out our programme for Dirichlet L-functions [6] using the Hardy-Littlewood conjecture, and for higher-order correlation functions using a new approach based on the universality of random-matrix correlations [7].

One of the most subtle aspects of the connection between number theory and random matrix theory is the interplay between arithmetic and universality; these play a complementary role in many of the formulae. It is a major challenge to understand this better. We have sought to do this by analysing the shifted moments and ratios of function-field L-functions. These had not previously been explored in this context. We proved several formulae for the shifted moments in [1] and [2]. In [3] we developed general conjectures for the shifted moments and ratios that predict exactly how the arithmetical and universal (random-matrix) components intertwine. We see this as a significant step forward. Our general expressions have attracted considerable attention; see, for example [29].

3 Further Research Directions

Our research went in several other directions directly related to those described above.

Together with Andrew Booker and Ghaith Hiary, JPK developed a new application of Random Matrix Theory to testing whether numbers are squarefree (without having to factorize them!). This had been a major challenge in Number Theory and we consider our alogorithm to be a significant achievement. It uses a relationship between squarefree integers and the low-lying zeros of certain L-functions. Random Matrix Theory describes the distribution of these low-lying zeros and so determines the efficiency of our algorithm. One application was to proving that the first RSA challenge number not yet factorised (RSA-210) is not square-full. Our paper [8] was recently accepted for publication in Duke Mathematical Journal.

A second direction that we find particularly exciting is a new idea that JPK and Brian Conrey are currently developing. This concerns one of the most famous puzzles in the subject: how do number-theoretic correlations give rise to the moment formulae predicted by Random Matrix Theory? The standard correlations that have been (very extensively) studied for the past hundred years clearly give the wrong answer;

for example, they predict negative values for the moments of the Riemann zeta-function beyond the eighth, when we know these values must, in fact, be positive. We now believe we have understood how to explain this puzzle – we have identified a new class of correlations whose importance had previously been overlooked. Preliminary calculations give us real hope that these resolve the problem. This would be a very significant step forward, if it proves correct. A first paper has already been written [10] and others are in preparation.

Another direction that we have explored concerns the probability of L-functions taking extremely large values. For the Riemann zeta function this is an old and highly contentious issue and there are a number of mutually contradictory conjectures. For elliptic curves it relates to the problem of understanding the probability of a given curve having an exceptionally large rank. We developed a model based on calculating when the characteristic polynomials of random matrices take exceptionally large values. Surprisingly, it turns out that this calculation is strikingly similar to that relating to how glasses freeze in statistical mechanics. Our conclusion is that the values of the Riemann zeta function and the characteristic polynomials of random matrices freeze and that this freezing fixes the probability of exceptionally large values appearing. We have published this work in a high-profile Letter [16] and in a longer paper that sets out our ideas in detail [17]. We again see this discovery as opening up several new avenues for further research. In particular, developing a quantitative understanding of the probability of curves having large ranks would have a very major impact. We believe this idea gives significant new insight into the question of extreme values.

To illustrate this we show in Figure 3 the results of a comparison of the prediction for the probability distribution of the largest value of the characteristic polynomial of a random unitary matrix, obtained using the freezing conjecture, with data from numerical experiments performed using randomly generated matrices of dimension $N = 50$. Similarly, in Figure 4 we show the theoretical curve together with numerical data obtained from computations of the Riemann zeta-function high on its critical line. The agreement is, we believe, noteworthy.

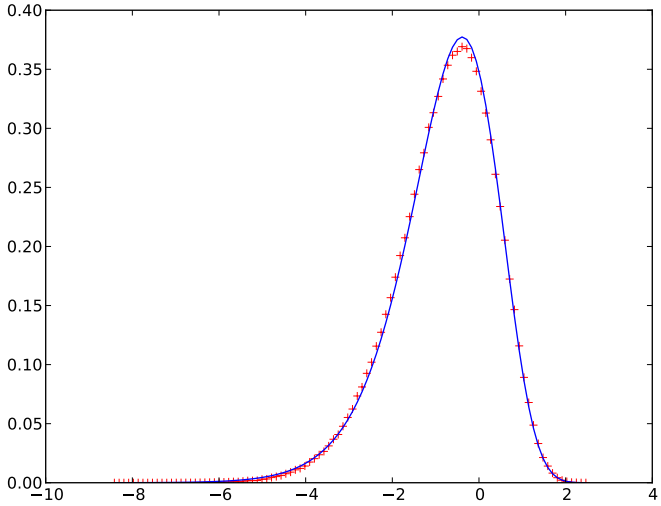

Figure 3: Comparison of the conjectured probability distribution of the supremum of the characteristic polynomial of random unitary matrix (blue line) with data (red crosses) from 106 random unitary matrices of dimension $N = 50$.

Underpinning all of our work is a philosophy that there may be a spectral interpretation of the zeros of L-functions, for example the Riemann zeta-function. This idea goes back to Hilbert and Polya. Establishing such an interpretation is one route to proving the Riemann Hypothesis, which is arguably the most important open problem in mathematics. The success of random-matrix models in describing the statistics of the zeros is evidence in favour of such an interpretation. However, Random Matrix Theory alone cannot predict what the operator might be whose eigenvalues are the zeros. The search for such an operator has driven research for nearly 100 years. Of course, we still have no idea whether such an operator exists, let alone what it might look like. But we have made progress in recent years in analysing certain candidates. In [5], Sir Michael Berry and JPK looked at one candidate and proved that its eigenvalues have the same mean density as the Riemann zeros. We know this is far from the end of the story, but this is the first truly self-adjoint candidate

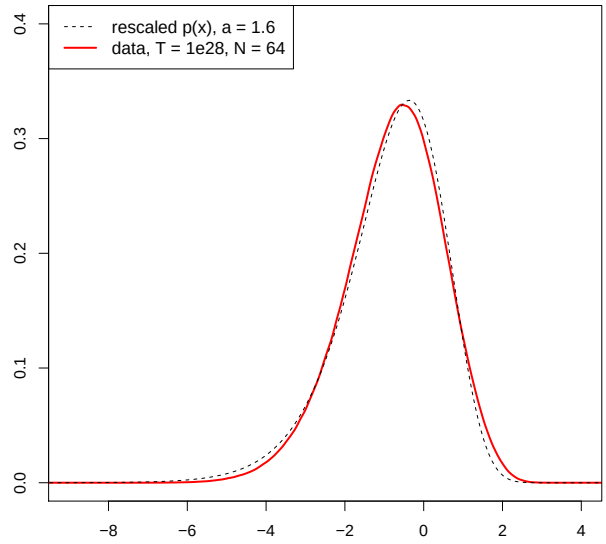

Figure 4: Comparison of the conjectured probability distribution of the supremum of the characteristic polynomial of random unitary matrix (black dashed line) with a numerical computation (solid red line) of the distribution of values of the supremum of the Riemann zeta function over an interval $T \leq t \leq T + 2\pi$ with T varying over a range containing 268 million zeros near to the height $T = 1028$ (corresponding to $N = 64$).

operator for which we know this to be true.

Finally, in collaboration with Manjul Bhargava (awarded a Fields' Medal in 2014), John Cremona, Tom Fisher and Nick Jones, JPK has established a new approach to the long-standing problem of determining the probability that a random quadratic form in many variables is indefinite. Essentially, by choosing the probability measure on the space of quadratic forms appropriately, we can map the problem onto an integrable random matrix calculation and so compute explicit formulae. We see our key idea – using a probability measure that allows for analytical calculations based on random-matrix methods – as having significantly wider applicability in this area.

4 Outputs and Evidence of their Impact

The main outputs of our research are ideas. We believe some of these to be significant. Most are contained in the following papers [1, 2, 3, 4, 5, 6, 7, 8, 10, 13, 14, 15, 16, 17, 21, 22, 26] and in several papers currently in preparation. We acknowledge EOARD support in all of these papers. In addition, JPK wrote a review of Random Matrix Theory for the Princeton Companion to Applied Mathematics [20], which will appear in 2015.

The following evidences the impact of our work

- NCS was an organiser of a semester programme at the Mathematical Sciences Research Institute (MSRI), Berkeley, on Arithmetic Statistics which focused on many of the areas covered by this grant.
- NCS gave an invited lecture on random matrix models for elliptic curves at the Hausdorff Center for Mathematics in Bonn, Germany in their conference: Emerging Leaders and Evolving Frontiers in Analytic Number Theory (ELEFANT), July 14 - 18, 2014.
- NCS will give an Plenary lecture on random matrix models for elliptic curves at the combined meeting of the Australian and New Zealand mathematical societies Melbourne, Australia, December 8-12, 2014.
- NCS gave an invited lecture on random matrix models for elliptic curves to the London Mathematical Society on July 4th 2014.

- JPK was awarded a Royal Society Wolfson Research Merit Award and a Royal Society Leverhulme Research Fellowship in 2014 in recognition of his work in the area supported by this grant.

- Our work on arithmetic statistics in function fields was a focal point of a workshop run at the American Institute of Mathematics in Palo Alto in January 2014. JPK gave a Keynote lecture at the meeting. It was also a focal point of a Royal Society Workshop at Chicheley Hall in May 2014 (of which JPK was the main organizer). Associated with the Chichely meeting will be a special volume of the Philosophical Transactions of the Royal Society (the world's oldest scientific journal).

- Our work on arithmetic statistics in function fields was also the subject of Zeev Rudnick's invited lecture at the International Congress of Mathematicians in August 2014, and it will be the subject of an invited lecture by JPK at a conference in honour of Peter Sarnak, in Princeton in December 2014.

- Our work on extreme values and freezing was a focal point of a workshop held at the Institute for Advanced Study, Princeton in November 2013, where JPK gave an invited lecture. JPK also gave a lecture on this subject at the Mathematical Sciences Research Institute, Berkeley, in April 2011, when he held the Eisenbud Visiting Chair.

- JPK gave a Distinguished Lecture Series on Random Matrix Theory and Number Theory at Baylor University Texas in November 2013, and will give a similar series of lectures at the Courant Institute New York in February 2015.

5 Use of Support

We are most grateful to the EOARD for supporting the research outlined above. Our view is that we have achieved the major objectives of our proposal, and that some unexpected discoveries (especially relating to freezing) have opened up highly promising new opportunities. We are especially grateful for the extension to the grant that enabled us to make the most of the funding we received. It is clear to us that the funding we received has contributed very significantly to accelerating progress in our work.

We used the funds to support several visitors who worked with us, including Eugene Bogomolny (Paris), Chantal David (Montreal), Eduardo Dueñez (San Antonio), Steven J. Miller (Williams), Nick Katz (Princeton), Mike Rubinstein (Waterloo), Zeev Rudnick (Tel Aviv), German Sierra (Madrid), Kannan Soundararajan (Stanford). We also funded a number of summer students and a PhD student. Finally, we purchased high-end computers which enabled our numerical experiments. These experiments included the computation of zeros on the critical line of the Riemann zeta-function higher up than ever previously reached – so the support led to a new world-record for the verification of the Riemann Hypothesis.

References

[1] J.C. Anadrade and J.P. Keating, The mean value of L(1/2, ?) in the hyperelliptic ensemble, *J. Number Theory* **132**: 2793–2816, 2012.

[2] J.C. Anadrade and J.P. Keating, Mean value theorems for L-functions over prime polynomials for the rational function field, *Acta Arithmetica* **161**: 371–385, 2013.

[3] J.C. Anadrade and J.P. Keating, Conjectures for the integral moments and ratios of L-functions over function fields, *J. Number Theory* **142**: 102–148, 2014.

[4] M. Bhargava, J. Cremona, T. Fisher, N.G. Jones and J.P. Keating, What is the probability that a random integral quadratic form in n variables is isotropic? submitted for publication.

[5] M.V. Berry and J.P. Keating, A compact hamiltonian with the same asymptotic mean spectral density as the Riemann zeros, *J. Phys. A* **44**, 285203, 2011.

[6] E.B. Bogomolny and J.P. Keating, Two-point correlation function for Dirichlet L-functions, *J. Phys. A* **46**, 095202, 2013.

[7] E.B. Bogomolny and J.P. Keating, A method for calculating spectral statistics based on random-matrix universality with an application to the three-point correlations of the Riemann zeros, *J. Phys. A* **46**, 305203, 2013.

[8] A.R. Booker, G.A. Hiary and J.P. Keating, Detecting squarefree numbers, *Duke Math. J.*, accepted for publication, in press.

[9] J.B. Conrey, Notes on eigenvalue distributions for the classical compact groups. In F. Mezzadri and N.C. Snaith, editors, *Recent Perspectives in random matrix theory and number theory*, pages 111–146. Cambridge University Press, 2005.

[10] J.B. Conrey and J.P. Keating, Moments of zeta and corrleations of divisor-sums: I submitted for publication.

[11] J.B. Conrey, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions, In *Number Theory for the Millennium I: Proceedings of the Millennial Conference on Number Theory*; editor, M.A. Bennett et al., pages 301–315. A K Peters, Ltd, Natick, 2002.

[12] J.B. Conrey, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, Random matrix theory and the Fourier coefficients of half-integral weight forms, *Experiment. Math.*, **15**(1):67–82, 2006.

[13] J.B. Conrey and N.C. Snaith.On the orthogonal symmetry of L-functions of a family of Hecke Grossencharacters. *Acta Arithmetica*, 157(4):323–356, 2013.

[14] J.B. Conrey and N.C. Snaith, In Support of n-Correlation *Commun. Math. Phys.*, 330(2): 639–653, 2014.

[15] E. Dueñez, D. K. Huynh, S. J. Miller, J. P. Keating, and N. C. Snaith, A random matrix model for elliptic curve L-functions of finite conductor, *J. Phys. A* **45**(11), 2012.

[16] Y.V. Fyodorov, G.A. Hiary and J.P. Keating, Freezing transition, characteristic polynomials of random matrices, and the Riemann zeta-function, *Phys. Rev. Lett.* **108**, 20120503, 2014.

[17] Y.V. Fyodorov and J.P. Keating, Freezing transitions and extreme values: random matrix theory, $\zeta(1/2+it)$, and disordered landscapes, *Phil. Trans. Roy. Soc. Lond.* **372**, 170601, 2012.

[18] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture. *Invent. Math.* **72**(2):241–265, 1983.

[19] N.M. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, Rhode Island, 1999.

[20] J.P. Keating, Random Matrix Theory, to appear in the Princeton Companion to Applied Mathematics.

[21] J.P. Keating and Z. Rudnick, The Variance of the Number of Prime Polynomials in Short Intervals and in Residue Classes, *International Mathematics Research Notices* **2014**, 259–288, 2014

[22] J.P. Keating and Z. Rudnick, Squarefree polynomials and Möbius values in short intervals and arithmetic progressions, submitted for publication.

[23] J.P. Keating and N.C. Snaith, Random matrix theory and L-functions at $s = 1/2$, *Comm. Math. Phys* **214**:91–110, 2000.

[24] J.P. Keating and N.C. Snaith, Random matrix theory and $\zeta(1/2+it)$, *Comm. Math. Phys.* **214**:57–89, 2000.

[25] W. Kohnen and D. Zagier, Values of L-series of modular forms at the center of the critical strip, *Invent. Math.* **64**:175–198, 1981.

[26] A.M. Mason and N.C. Snaith Orthogonal and Symplectic n-level densities, submitted for publication

[27] S.J. Miller, Investigations of zeros near the central point of elliptic curve L-functions (appendix by E. Dueñez), *Experiment. Math.* **15**(3):257–79, 2006.

[28] F. Rodriguez-Villegas and D. Zagier. Square roots of central values of Hecke L -series. In *Advances in number theory (Kingston, ON, 1991)*, page 8199. Oxford Sci. Publ., Oxford Univ. Press, New York, 1993.

[29] M.O. Rubinstein and K. Wu Moments of zeta functions associated to hyperelliptic curves over finite fields http://arxiv.org/pdf/1407.1018.pdf

[30] Z. Rudnick and P. Sarnak, Zeros of principal L-functions and random matrix theory. *Duke Math. J* 81:269–322, 1996.

[31] G. Shimura, On modular forms of half integral weight, *Ann. of Math.* **97**(2):440–481, 1973.

[32] J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* **60**(9):375–484, 1981.